Insider Threats Involving Supply Chain Risk

A Sneak Peak of the CERT National Insider Threat Center's Incident Corpus

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-1206

A Note About the Cases

The statistics and figures represented in the remaining slides are limited to:

- Domestic incidents with publicly available information
- Malicious insiders
- Cases identified as Fraud, Sabotage, Theft of IP, and / or Misuse

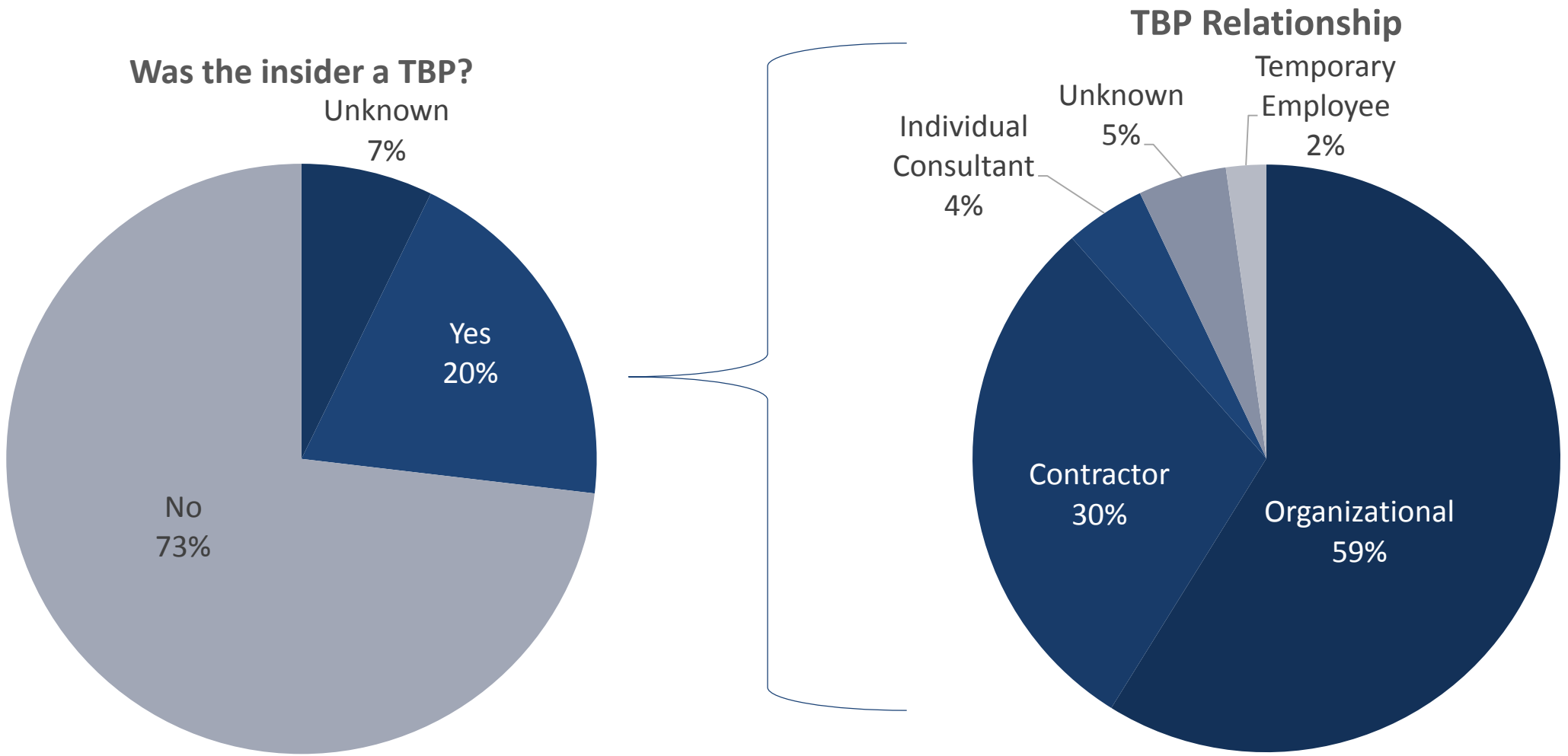
The incidents included in the CERT Insider Threat Incident Corpus were successfully detected and, by and large, led to a criminal or civil legal action. Therefore, these statistics do not represent malicious insiders that were able to entirely circumvent detection.

Analysis of the CERT Insider Threat Incident Corpus is dynamic, so categories and definitions are subject to change over time.

Insider Threats Involving Supply Chain Risk

Statistics

Trusted Business Partners TBP



Insider Threats Involving Supply Chain Risk

Case Examples

Case Example: IT Sabotage #1

A contractor has their access to their employer's facility disabled following a dispute.

This insider, a subcontractor at an energy management facility, did not have their access terminated at the victim organization.

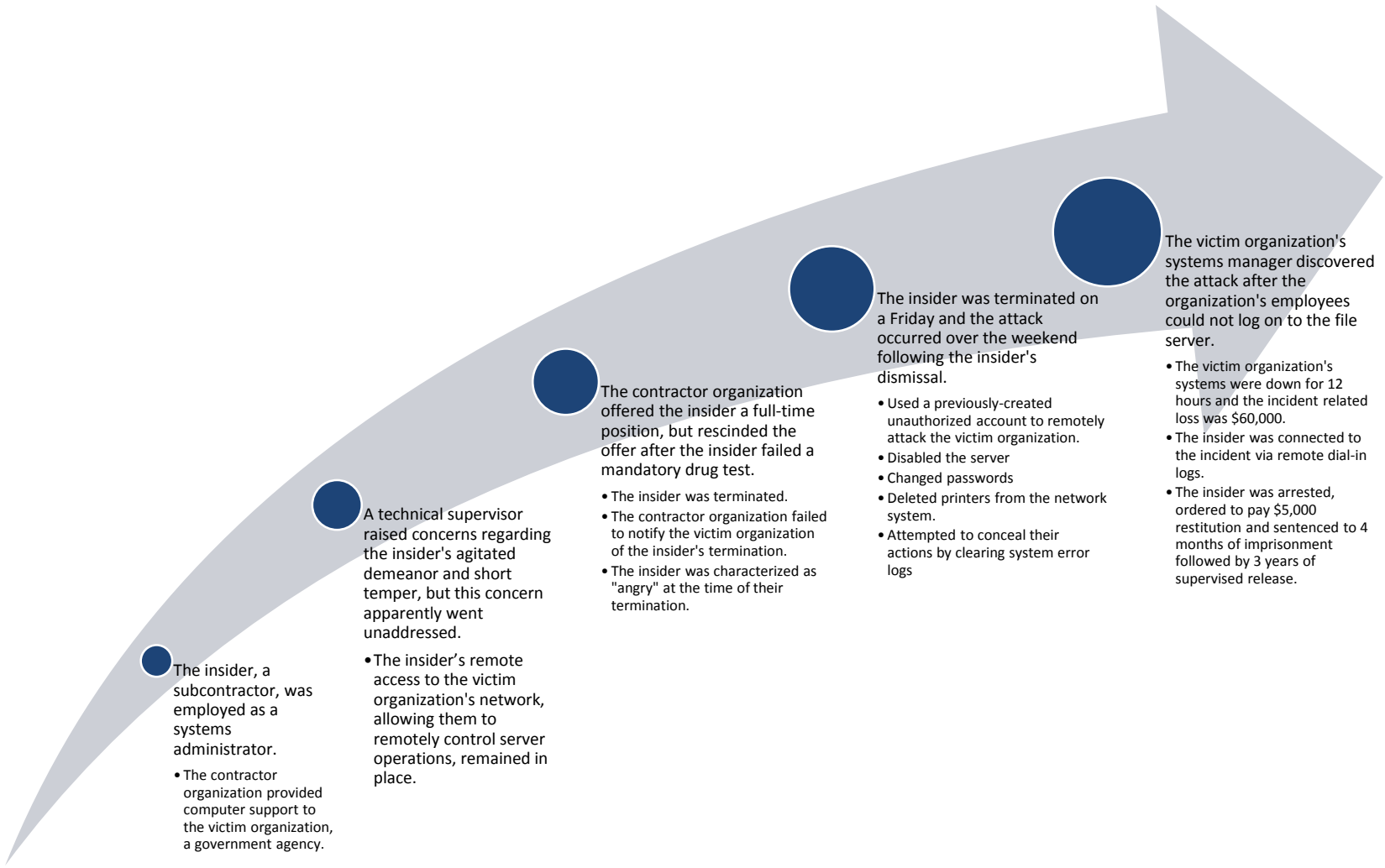
- The insider breaks the glass enclosing the emergency power button.

The insider then shuts down computers that regulate the exchange of electricity between power grids.

As a result, there is:

- An internal power outage
- Shutdown of electricity between the power grids in the US

Case Example: IT Sabotage #2



The insider, a subcontractor, was employed as a systems administrator.

- The contractor organization provided computer support to the victim organization, a government agency.

A technical supervisor raised concerns regarding the insider's agitated demeanor and short temper, but this concern apparently went unaddressed.

- The insider's remote access to the victim organization's network, allowing them to remotely control server operations, remained in place.

The contractor organization offered the insider a full-time position, but rescinded the offer after the insider failed a mandatory drug test.

- The insider was terminated.
- The contractor organization failed to notify the victim organization of the insider's termination.
- The insider was characterized as "angry" at the time of their termination.

The insider was terminated on a Friday and the attack occurred over the weekend following the insider's dismissal.

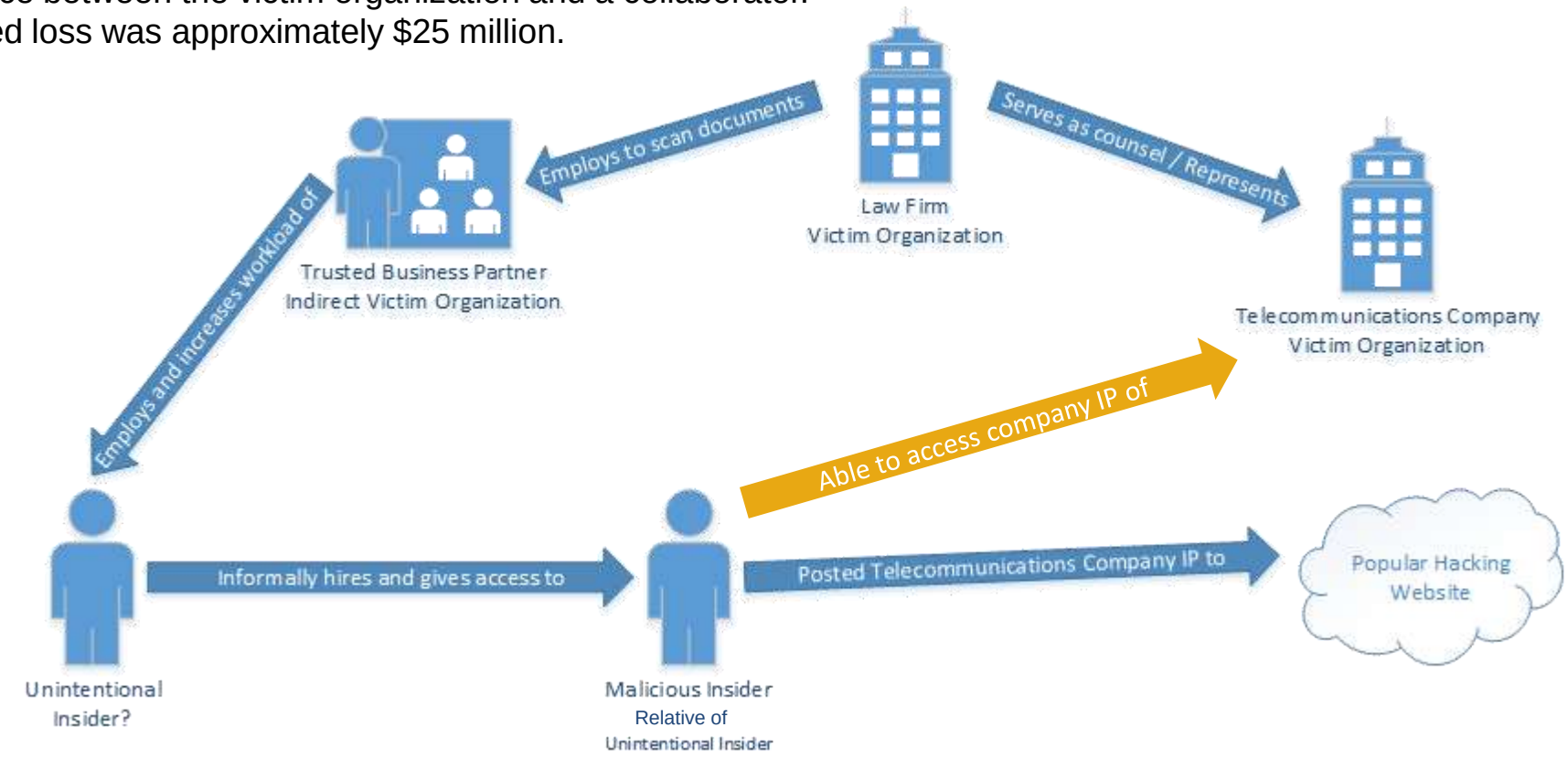
- Used a previously-created unauthorized account to remotely attack the victim organization.
- Disabled the server
- Changed passwords
- Deleted printers from the network system.
- Attempted to conceal their actions by clearing system error logs

The victim organization's systems manager discovered the attack after the organization's employees could not log on to the file server.

- The victim organization's systems were down for 12 hours and the incident related loss was $60,000.
- The insider was connected to the incident via remote dial-in logs.
- The insider was arrested, ordered to pay $5,000 restitution and sentenced to 4 months of imprisonment followed by 3 years of supervised release.

Case Example: Theft of IP

A contractor was unofficially working for the company's TBP, a document imaging company. The victim organization was a high technology company. The TBP was hired to copy trade secrets in preparation for litigation. The malicious insider was hired informally by a family member to assist with the high workload. The insider stole and posted trade secrets, design notes, and correspondence between the victim organization and a collaborator. The incident related loss was approximately $25 million.

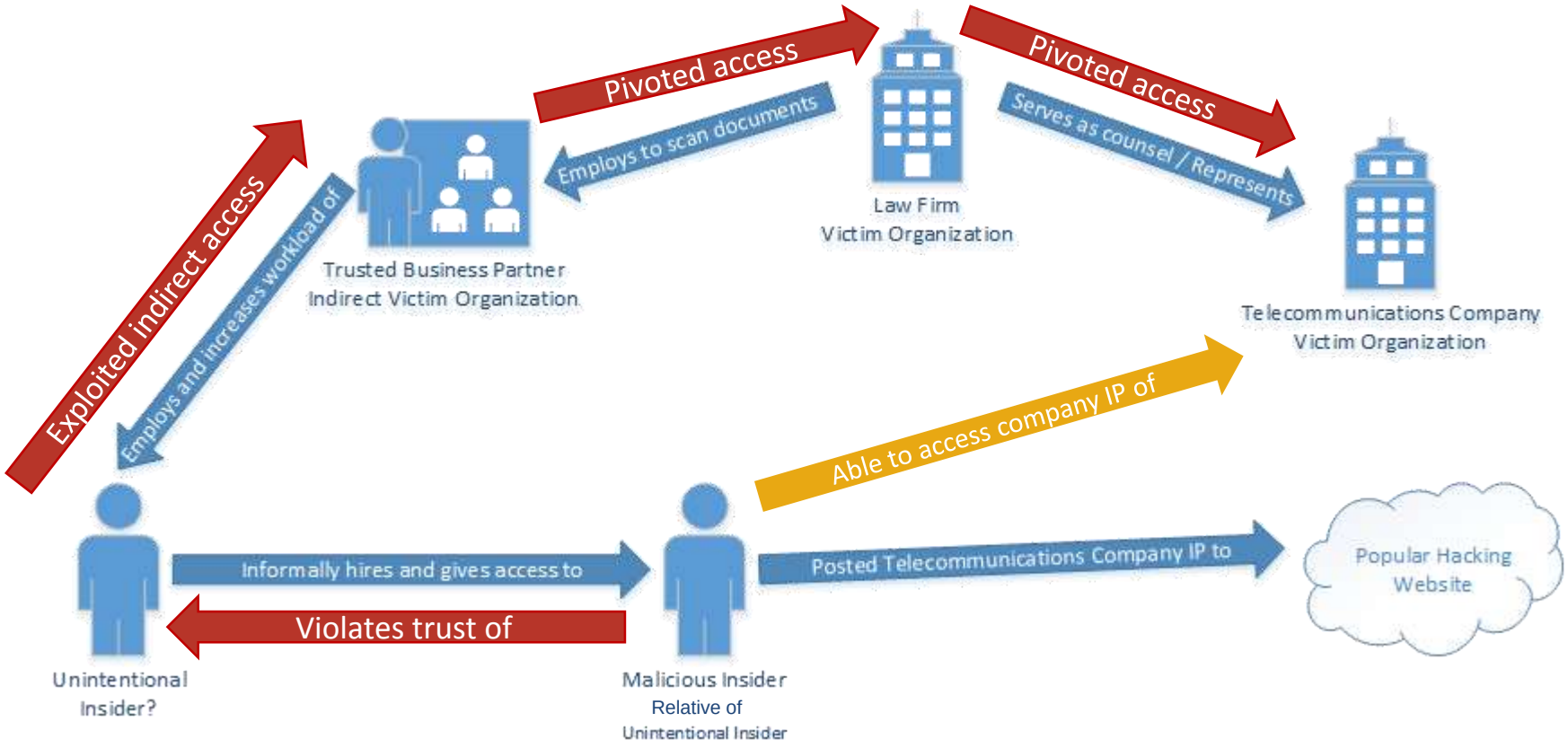


Unintentional Insider Unwittingly Facilitated Theft of IP

- Overwhelmed employee
- Informally hired family member to help with workload
- Provided access to family member that was granted by their employer to sensitive legal documents and IP
- May or may not have been aware that family member had taken documents home with them to scan them as requested
- May or may not have been aware of family member's connection to online hacking community

Malicious Insider

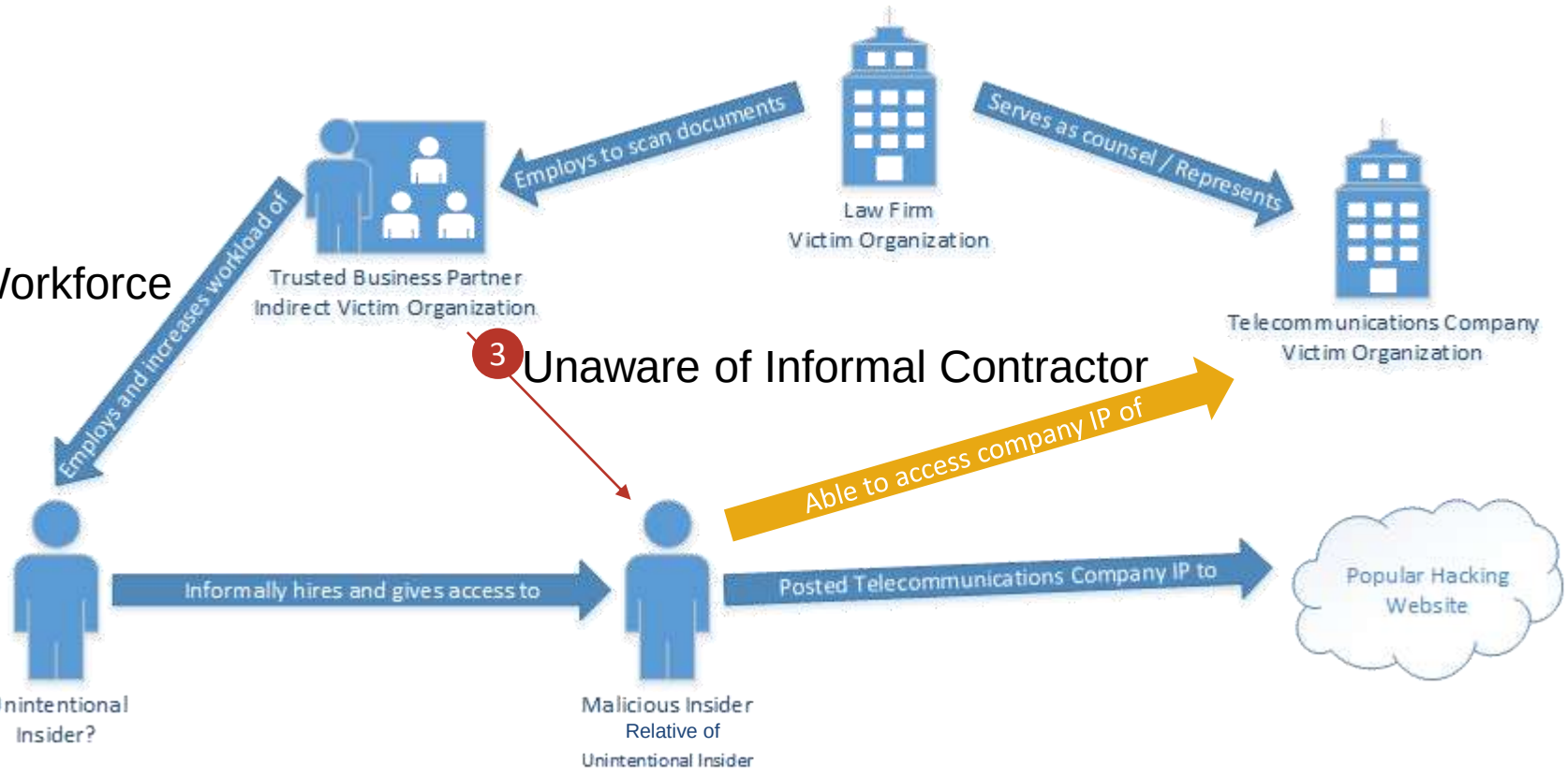
The malicious insider violated the access provided to them on a number of levels.



Lessons Learned for TBP Organization

The incident suggests a number of organizational issues across the different entities involved. Three issues stand out in particular for the Trusted Business Partner.

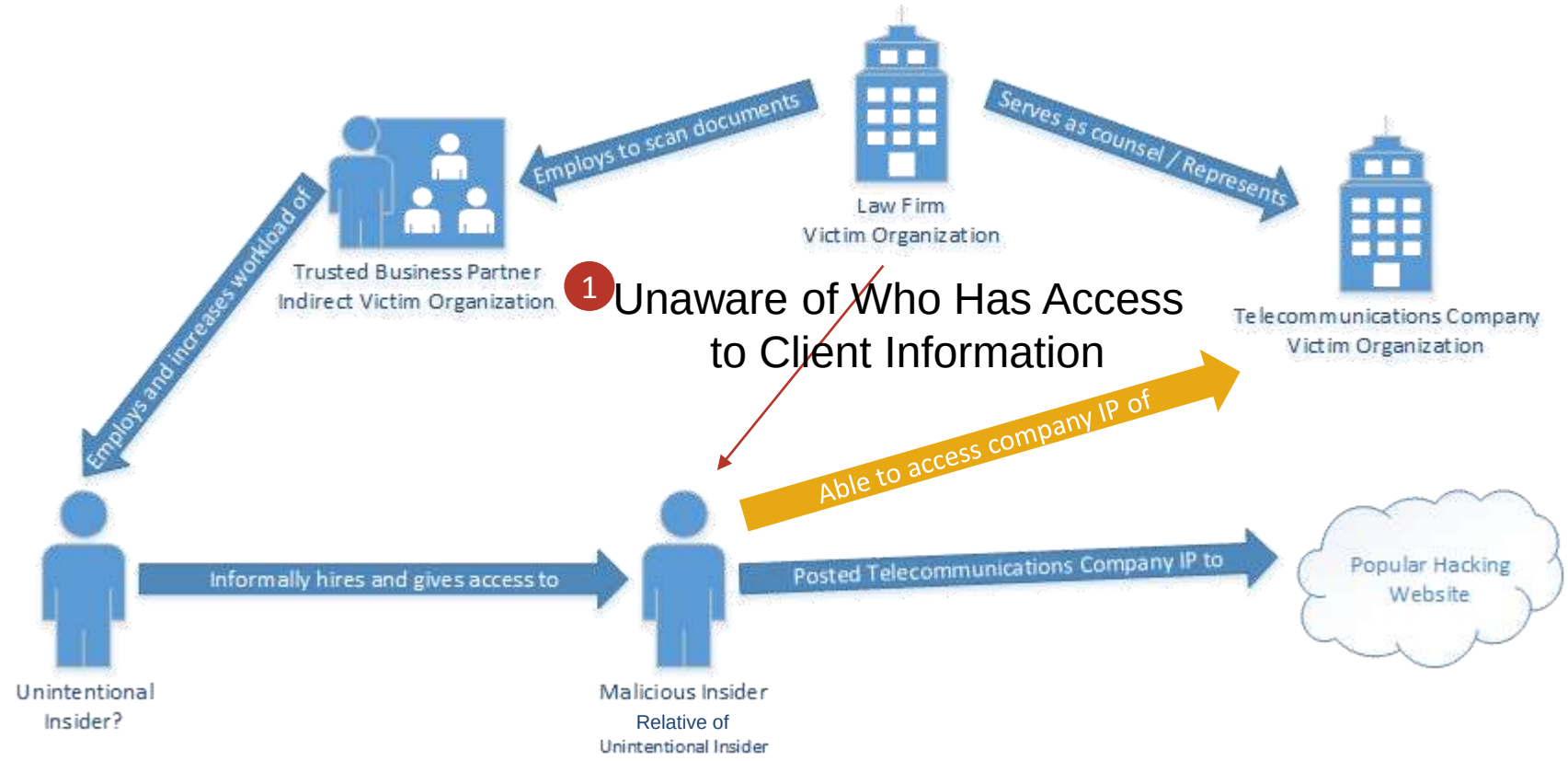
1 Overextended Workforce



2 Employee Hired Informal Contractor

Lessons Learned for Victim Organization

The incident suggests a number of organizational issues across the different entities involved. An additional issue stands out for the Law Firm Victim Organization.



Insider Threats Involving Supply Chain Risk

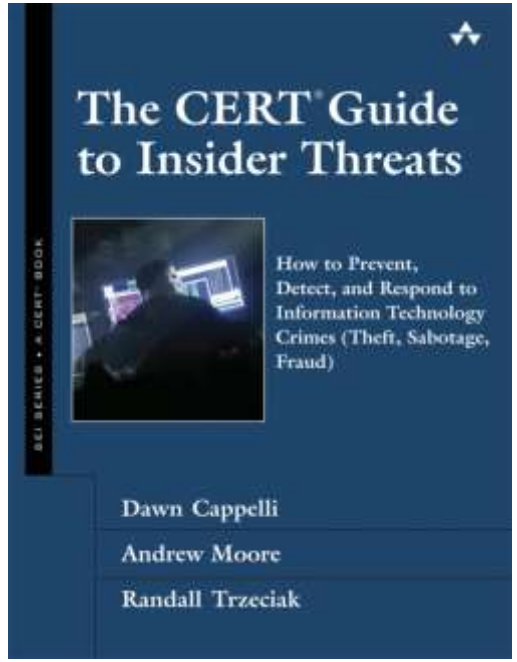
Additional Information

NITC Publications and References

Theis, M. C., Trzeciak, R. F., Costa, D. L., Moore, A. P., Miller, S., Cassidy, T., & (2019) Claycomb, W. R. Common Sense Guide to Mitigating Insider Threats (6th Ed.). Pittsburgh: Software Engineering Institute.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley Professional.

Moore, Andrew; Savinda, Jeff; Monaco, Elizabeth; Moyes, Jamie; Rousseau, Denise; Perl, Samuel; Cowley, Jennifer; Collins, Matthew; Cassidy, Tracy; VanHoudnos, Nathan; Buttles-Valdez, Palma; Bauer, Daniel; & Parshall, Allison. The Critical Role of Positive Incentives for Reducing Insider Threats. CMU/SEI-2016-TR-014. Software Engineering Institute, Carnegie Mellon University. 2016.



For More Information

Software Engineering Institute (SEI)

National Insider Threat Center	http://www.cert.org/insider-threat/
National Insider Threat Center Email	insider-threat-feedback@cert.org
Insider Threat Blog	http://insights.sei.cmu.edu/insider-threat/
SEI Digital Library	https://resources.sei.cmu.edu/library/

SANS Institute

Combatting Cyber Risks in the Supply Chain (White Paper):

https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_273005.pdf

Contact Information

Point of Contact

Sarah Miller

Insider Threat Researcher

CERT National Insider Threat Center

Email: semiller@cert.org

For Industry Organizations Only

Open Source Insider Threat Information Sharing Group (OSIT)

Data Analytics Special Interest Group (DA SIG)

Email: osit-forum-support@cert.org

Privacy Special Interest Group

Email: privacy-sig-owner@cert.org